COL872-Assignment 1

Secret Sharing without a trusted party (Dealer)

Due Date: 14th Sept 2022 at 11:59 PM

Release Date: 30-08-2022

Introduction: Security in cryptography is based on the secret key k. Suppose in an organization there are total n employees. Out of these n, n_1 employees are privileged employees or you can say owner. So, there are $n_2 = n - n_1$ other employees.

Now, in order to create a secret, it is needed that at least 1 owner and total t (minimum) employees are needed which may/may not be owner. Assume $t > n_1$ and there is no dealer.

Let p be a safe prime and g be the generator of Z_p^*. p and g are public parameters.

The secret $k \in Z_p^*$ should be stored as $h = g^k \bmod p$.

There should be three separate programs:

1. Creation of secret and finding $h = g^k \bmod p$ (the value to be stored)
2. Master Secret Share Generation
3. Verification of the secret by min t participants

Programming language may python or MATLAB or C/C++.